



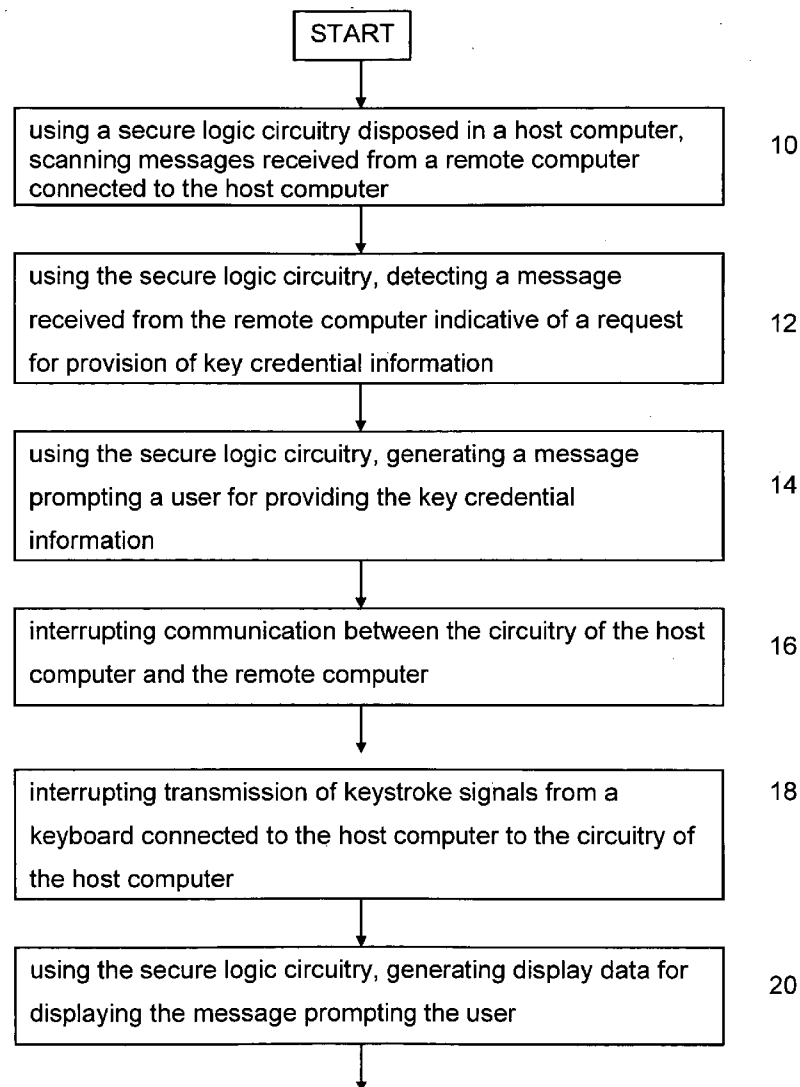
US 20100186070A1

(19) **United States**(12) **Patent Application Publication**
McAlear(10) **Pub. No.: US 2010/0186070 A1**(43) **Pub. Date: Jul. 22, 2010**(54) **SYSTEM, DEVICE AND METHOD FOR
SECURE PROVISION OF KEY CREDENTIAL
INFORMATION****Publication Classification**(51) **Int. Cl.**
H04L 9/32 (2006.01)
G06F 15/16 (2006.01)
(52) **U.S. Cl.** **726/5**(76) **Inventor: James A. McAlear, Ottawa (CA)**(57) **ABSTRACT**

Correspondence Address:

Frank J. Bonini, Jr.**Harding, Earley, Follmer & Frailey****P.O. Box 750****Valley Forge, PA 19482-0750 (US)**

A system for secure provision of key credential information is provided. The system comprises secure logic circuitry for being disposed in a host computer. The secure logic circuitry detects a message received from a remote computer connected to the host computer and indicative of a request for provision of the key credential information; generates a message for prompting a user for provision of the key credential information; receives the key credential information; and provides the key credential information to the remote computer absent processing using circuitry of the host computer. The system further comprises a secure user interface connected to the secure logic circuitry for receiving the key credential information from the user and providing the same to the secure logic circuitry.

(21) **Appl. No.: 12/321,519**(22) **Filed: Jan. 22, 2009**

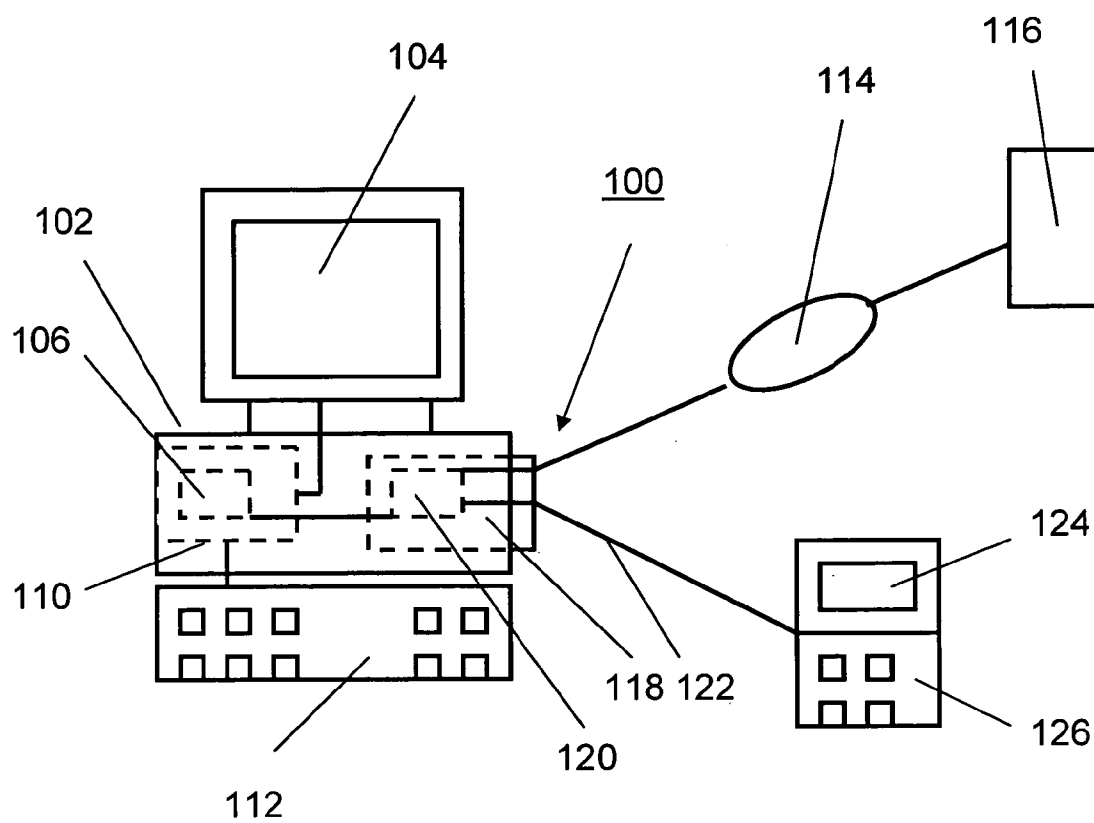


Figure. 1A

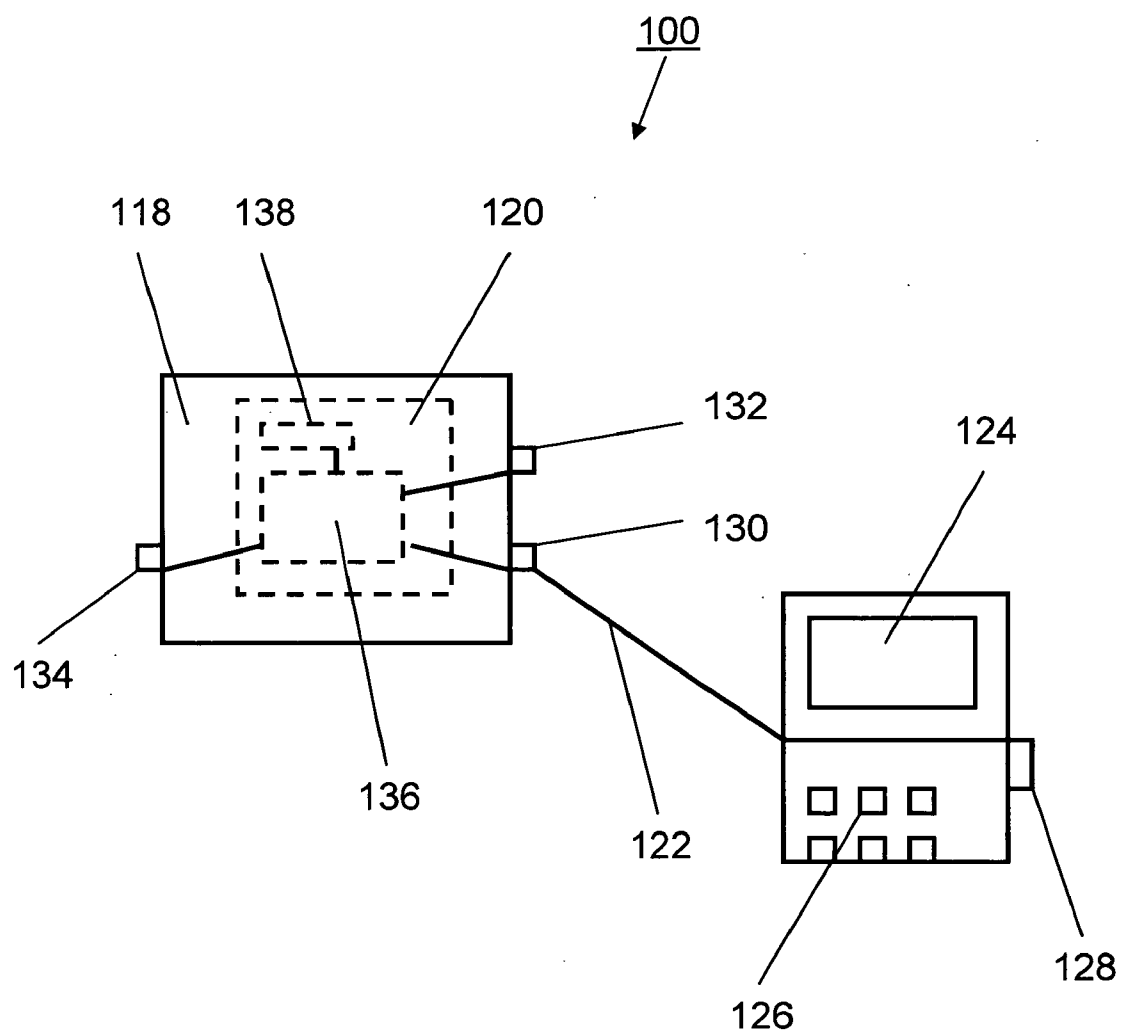
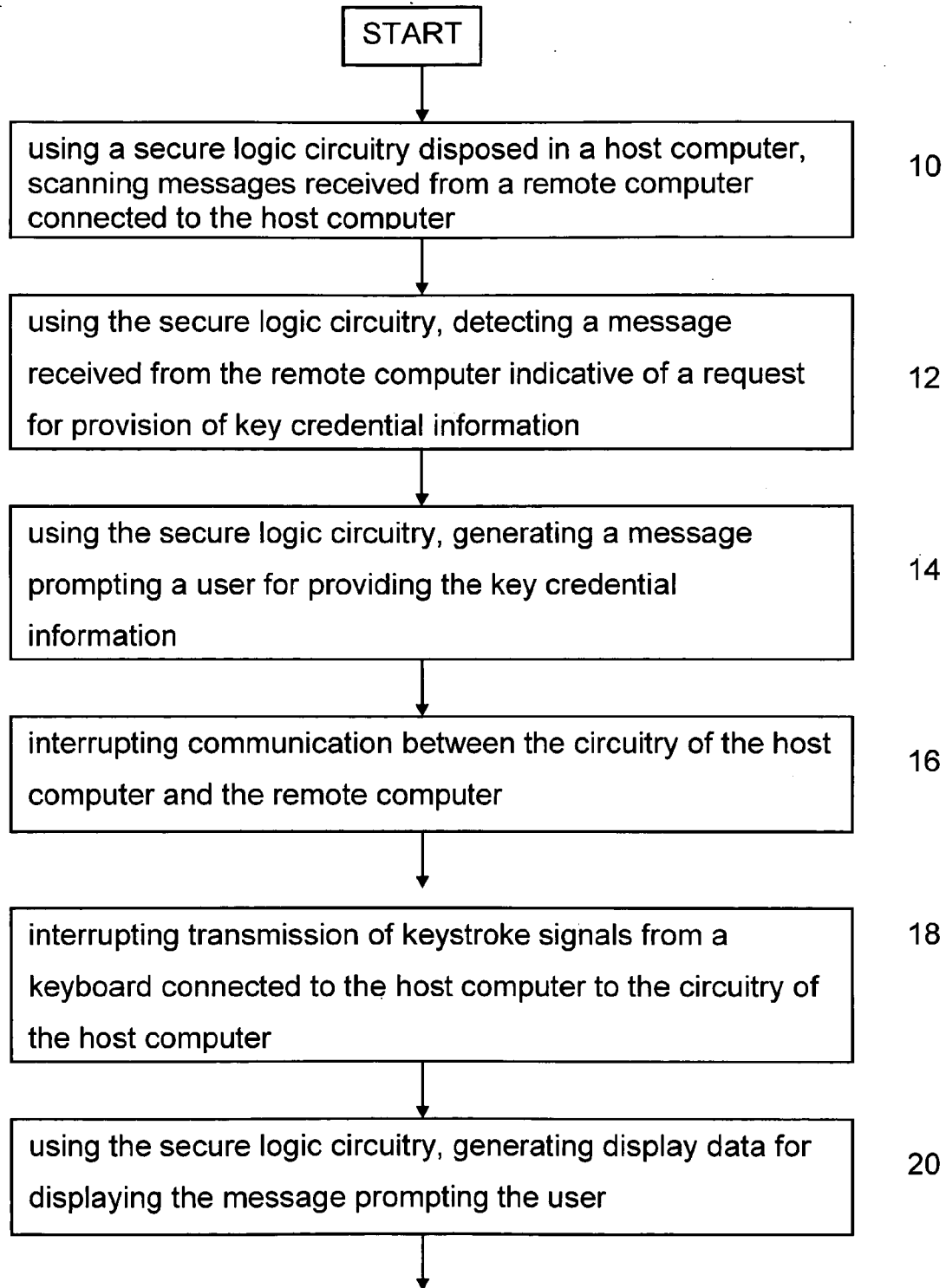
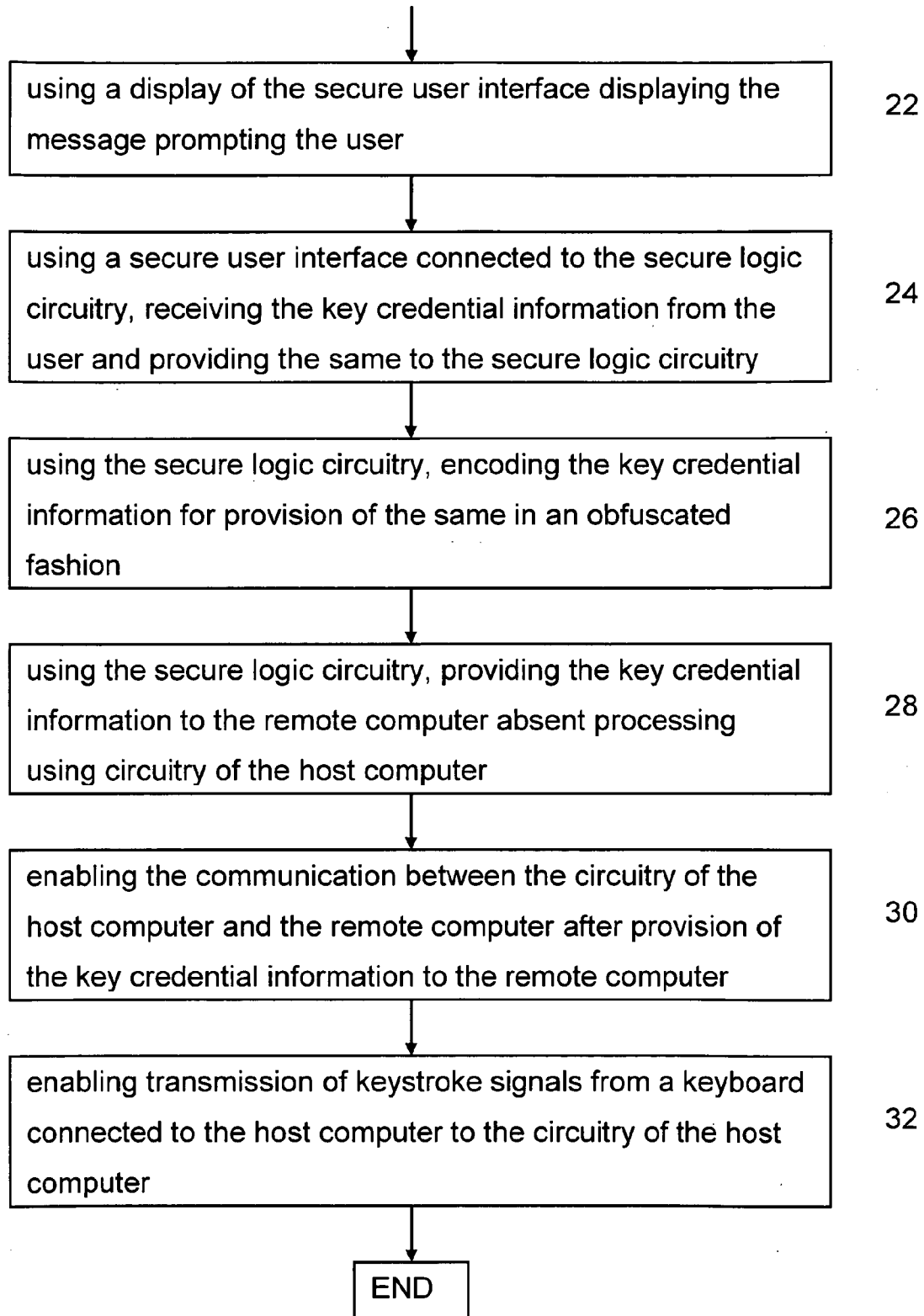


Figure. 1B

**Fig. 2**

**Fig. 2 continued**

SYSTEM, DEVICE AND METHOD FOR SECURE PROVISION OF KEY CREDENTIAL INFORMATION

BACKGROUND OF THE INVENTION

[0001] 1. Field of the Invention

[0002] The present invention relates to computer networking, and more particularly to a system for secure provision of key credential information to a server via an un-trusted computer.

[0003] 2. Brief Description of the Related Art

[0004] Commerce over the Internet has become very popular. Such commerce takes many forms, from purchasing merchandise from online vendors to conducting online banking and stock trading. Common to all such transactions is the need to transmit private secure information. Typically, the transactions are carried out using secure encrypted connections. However, there are still opportunities to capture the private information that is used during online transactions, for example, to obtain passwords, Personal Identification Numbers (PIN), social security numbers, driver's license numbers and account numbers, to name a few. Illegal procurement of such information and using the same in a fraudulent manner is commonly referred to as identity theft.

[0005] While the Internet is by far the largest and most pervasive computer network, the problem of identity theft occurs in other networks as well. For example, identity theft can occur entirely within the confines of a corporate network or a university network wherein a dishonest individual uses a transaction within the network to steal PINs enabling access to confidential information.

[0006] Many of the current security mechanisms assume that a user's computer and its keyboard are secure, which is incorrect. One form of conducting online identity theft is to use a keystroke logger to log individual keystrokes for extracting personal information. The keystroke logger is, for example, software installed on a computer without the user's knowledge and its operation is invisible to the user. The keystroke logger in the form of software is, for example, distributed and installed remotely—for example, in the form of malware—and transmits the key logs to a remote computer in an invisible fashion. Numerous anti-virus programs fight known malicious software programs and try to keep up with the proliferation of new malicious software programs.

[0007] It is desirable to provide a system for secure provision of key credential information to a server via an un-trusted computer.

[0008] It is also desirable to provide a system for secure provision of key credential information that is easily installed in an existing computer system.

SUMMARY OF THE INVENTION

[0009] Accordingly, one object of the present invention is to provide a system for secure provision of key credential information to a server via an un-trusted computer.

[0010] Another object of the present invention is to provide a system for secure provision of key credential information that is easily installed in an existing computer system.

[0011] According to one aspect of the present invention, there is provided a system for secure provision of key credential information. The system comprises secure logic circuitry for being disposed in a host computer. The secure logic circuitry detects a message received from a remote computer

connected to the host computer which is indicative of a request for provision of the key credential information; generates a message for prompting a user for provision of the key credential information; receives the key credential information; and provides the key credential information to the remote computer absent processing using circuitry of the host computer. The system further comprises a secure user interface connected to the secure logic circuitry for receiving the key credential information from the user and providing the same to the secure logic circuitry.

[0012] According to another aspect of the present invention, there is further provided a method for secure provision of key credential information. Using a secure logic circuitry disposed in a host computer, a message received from a remote computer connected to the host computer which is indicative of a request for provision of the key credential information is detected. Using the secure logic circuitry, a message prompting a user for providing the key credential information is generated. Using a secure user interface connected to the secure logic circuitry, the key credential information is received from the user and provided to the secure logic circuitry. Using the secure logic circuitry, the key credential information is provided to the remote computer absent processing using circuitry of the host computer.

[0013] The advantage of the present invention is that it provides a system for secure provision of key credential information to a server via an un-trusted computer.

[0014] A further advantage of the present invention is that it provides a system for secure provision of key credential information that is easily installed in an existing computer system.

BRIEF DESCRIPTION OF THE DRAWINGS

[0015] A preferred embodiment of the present invention is described below with reference to the accompanying drawings, in which:

[0016] FIGS. 1A and 1B are simplified block diagrams of a system for secure provision of key credential information according to a preferred embodiment of the present invention; and,

[0017] FIG. 2 is a simplified flow diagram of a method for secure provision of key credential information according to a preferred embodiment of the present invention.

DESCRIPTION OF THE PREFERRED EMBODIMENT

[0018] Unless defined otherwise, all technical and scientific terms used herein have the same meaning as commonly understood by one of ordinary skill in the art to which the invention belongs. Although any methods and materials similar or equivalent to those described herein can be used in the practice or testing of the present invention, the preferred methods and materials are now described.

[0019] While the description of the preferred embodiments herein below is with reference to an Internet connection for sake of simplicity, it will become evident to those skilled in the art that the embodiments of the invention are not limited thereto, but are also applicable for use with various other networks such as, for example, corporate networks or university networks.

[0020] Referring to FIGS. 1A and 1B, a system for secure provision of key credential information **100** according to a preferred embodiment of the invention is provided. A user's Personal Computer (PC) or workstation **102** is connected via

a communication network **114** such as, for example, the Internet, to a remote computer **116**, for example, a server of an Internet based booking center or vendor. Typically, computers such as PCs and workstations communicate with the communication network **114** via a Network Interface Card (NIC) **118** which is connected to a motherboard **110** comprising a Central Processing Unit (CPU) **106** via an internal bus system. The user typically interacts with the computer **102** using key board **112** for providing information and commands to the CPU **106** and monitor **104** for visually receiving information, for example, in a graphical fashion.

[0021] The system for secure provision of key credential information **100** enables a user to communicate key credential information to the server **116** such that a malware having, for example, a surreptitious key logger capability, resident in the computer's CPU **106** or motherboard **110** is not able to see the provided key credential information.

[0022] The system for secure provision of key credential information **100** preferably comprises a NIC **118** having secure logic circuitry **120** connected to ports **130**, **132**, and **134**. The ports **132** and **134** are connected to the communication network **114** and the internal bus system of the computer **102**, respectively. The secure logic circuitry **120** comprises, for example, a processor **136** and memory **138** having executable commands stored therein for execution on the processor **136**. The secure logic circuitry **120** scans messages received from the server **116** for detecting a message which is indicative of a request for provision of the key credential information. Typically, when a user attempts to invoke a service on a remote network resource, the server then sends a request for credentials message to the computer **102**. For example, in conventional web browsing operations the CPU **106** of the computer **102** sends a HTTP GET message to the server **116** specifying a server resource and the server **116** replies with a HTTP **401** Authorization Required message with an embedded realm-title such as "Some-Service Login" to alert the user to exactly which set of key credentials are required for the requested resource.

[0023] When the secure logic circuitry **120** encounters a "request for key credentials" message the request is not passed to the computer motherboard **110**—as is using conventional technology—but instead is passed to a secure user interface **124**, **126** connected to the secure logic circuitry **120** via the port **130**. The secure user interface comprises, for example, a secure keyboard **126** for receiving the key credential information from the user and a secure display **124** for displaying a message for prompting the user for provision of the key credential information. Alternatively, the secure user interface comprises a touchscreen. The secure user interface is deployed, for example, as a peripheral device connected to the port **130** via cable **122**. Alternatively, wireless communication is enabled between the secure logic circuitry **120** and the secure user interface **124**, **126** using, for example, RF or infrared signal transmission techniques. For example, for common web browsing the secure logic circuitry **120** scans for messages coming from remote port **80** that contains the HTTP **401** message. More generally, a dedicated internet protocol is used to handle credentials for more general services or the secure logic circuitry **120** scans for authentication for each type of internet protocol, e.g. POP on port **110**. The secure logic circuitry **120** generates a message for prompting the user for provision of the key credential information which is then transmitted to the secure display **124** for alerting the user. Optionally, an audio alert is generated using, for

example, a loudspeaker disposed in the secure user interface. For example, for a common web browsing situation, the secure display shows the embedded realm title such as "Some-Service Login".

[0024] Optionally, the secure logic circuitry interrupts communication between the keyboard and the motherboard, for example, simultaneously when the message for prompting the user for provision of the key credential information is displayed.

[0025] Optionally, keyboard **126** can be enhanced with a second non-secured keyboard-to-PC connection link (not shown) that can transmit keystrokes from the enhanced keyboard **126** to the PC motherboard **110** in a non-secure mode, this optional enhanced keyboard **126** additionally having a user-activatable switch **128** that, when activated, temporarily blocks future transmission via the second non-secured keyboard-to-PC connection link to halt any typed keystrokes provided from the keyboard from reaching the motherboard **110**, and when activated, additionally temporarily allowing future transmission of data from the enhanced keyboard **126** to the NIC **118** via cable **122** or such other manner known to a person skilled in the art. This eliminates the requirement for the PC user to have separate secure and non-secure keyboards.

[0026] The user enters the required key credential information which is then sent to the secure logic circuitry **120** via cable **122**. Upon receipt, the secure logic circuitry **120** provides the key credential information to the remote computer **116** absent processing using the motherboard **110**, for example, by generating a reply message with the key credential information contained therein. Once the key credential information has been received, conventional communication and operation proceeds. For the common web browsing situation the secure logic circuitry **120** additionally keeps track of outgoing HTTP GET requests, because within the HTTP protocol, an authorization message is supplied by retrying the originals HTTP GET request with an additional Authorization field added that contains the key credential information.

[0027] As is evident, there are numerous variants for coding the key credential information. For example, the HTTP protocol defines a low security Basic mode, where the key credential information is transmitted over the network using a base-64 transfer encoding. HTTP also includes a Digest based authentication mechanism, whereby the HTTP **401** message also contains a one-time unique server supplied "salt" value. In this authentication technique, the authentication reply is a specified hash computation of the user key credential information and the "salt" value, for which the server evaluates the correctness. Using this technique, a network based eavesdropper is not able to recover the key credential information. Of course, there are numerous other methods for encoding the key credential information using various encryption techniques. The secure logic circuitry **120** is adaptable to perform these various encoding techniques in a straightforward manner.

[0028] The system for secure provision of key credential information **100** is easily installed, for example, in the form of a NIC, into an existing insertion slot of a computer such as a PC or workstation with the secure user interface being connected thereto, allowing retrofitting of existing computer systems in a simple fashion.

[0029] Referring to FIG. 2, a simplified flow diagram of a method for secure provision of key credential information according to a preferred embodiment of the invention is pro-

vided. The method is implemented using the system 100 described above. At 10, using the secure logic circuitry 120 disposed in the host computer 102 messages received from the remote computer 116 are scanned for detecting—12—a message received from the remote computer 116 which is indicative of a request for provision of key credential information. Upon detection of the message, the secure logic circuitry generates a message prompting a user for providing the key credential information—14. Optionally, the secure logic circuitry interrupts—16—communication between circuitry 110 of the host computer 102 and the remote computer 116 to increase security. At 18, transmission of keystroke signals to the circuitry 110 of the host computer 102 from a keyboard 112 connected to the host computer 102 is interrupted. The interruption is performed, for example, when a same keyboard connected to the motherboard 110 and to the secure logic circuitry 120 is used. For example, the user presses a toggle switch disposed on the keyboard prior provision of the key credential information. Alternatively, the interruption is performed automatically, using the secure logic circuitry 120. Optionally, the interruption is also performed when two separate keyboards or a touch screen are employed to prevent accidental use of the keyboard connected to the motherboard 110 for provision of the key credential information by the user.

[0030] At 20, the secure logic circuitry generates display data for displaying the message prompting the user which is then displayed—22—using the secure display 124. Using the secure user interface connected to the secure logic circuitry 120, the key credential information is received from the user and provided to the secure logic circuitry 120, at 24. Using the secure logic circuitry 120, the key credential information is encoded—26—using one of various available encoding techniques for providing the key credential information in an obfuscated fashion. The secure logic circuitry 120 then sends—28—the key credential information to the remote computer 116 absent processing using circuitry 110 of the host computer 102.

[0031] After provision of the key credential information to the remote computer 116 communication between the circuitry 110 of the host computer 102 and the remote computer 116 is enabled—30—as well as transmission of keystroke signals from the keyboard to the circuitry 110 of the host computer 102, at 32.

[0032] It is understood that in the preferred embodiment of the present invention, the NIC of the present invention would not incorporate or utilize a conventional packet sniffer function that would capture the secure credential packets being transmitted therethrough (to mitigate the risk that malware could locate and acquire such data from the NIC).

[0033] It is also understood that, in the case of a laptop computer, an NIC of the present invention may be provided which is physically separate from, and connectable to the laptop by way of, for example, a USB port or other interface on the laptop, in a manner known to a person skilled in art (network access to and from laptop thereafter being provided by way of the NIC of the present invention).

[0034] The present invention has been described herein with regard to preferred embodiments. However, it will be obvious to persons skilled in the art that a number of variations and modifications can be made without departing from the scope of the invention as described herein.

What is claimed is:

1. A system for secure provision of key credential information comprising:
 - secure logic circuitry for being disposed in a host computer, the secure logic circuitry for:
 - detecting a message received from a remote computer connected to the host computer and indicative of a request for provision of the key credential information;
 - generating a message for prompting a user for provision of the key credential information receiving the key credential information; and,
 - providing the key credential information to the remote computer absent processing using circuitry of the host computer; and,
 - a secure user interface connected to the secure logic circuitry for receiving the key credential information from the user and providing the same to the secure logic circuitry.
2. A system for secure provision of key credential information as defined in claim 1 wherein the secure user interface comprises:
 - a secure display for displaying the message for prompting the user for provision of the key credential information; and,
 - a secure keyboard for providing the key credential information.
3. A system for secure provision of key credential information as defined in claim 1 wherein the secure logic circuitry is placed on a network interface card.
4. A system for secure provision of key credential information as defined in claim 3 wherein the secure user interface is provided as a peripheral device connected to the network interface card.
5. A system for secure provision of key credential information as defined in claim 1 wherein the secure logic circuitry comprises a processor and memory, the memory having executable commands stored therein for execution on the processor.
6. A method for secure provision of key credential information comprising:
 - using a secure logic circuitry disposed in a host computer, detecting a message received from a remote computer connected to the host computer and indicative of a request for provision of the key credential information;
 - using the secure logic circuitry, generating a message prompting a user for providing the key credential information;
 - using a secure user interface connected to the secure logic circuitry, receiving the key credential information from the user and providing the same to the secure logic circuitry;
 - using the secure logic circuitry, providing the key credential information to the remote computer absent processing using circuitry of the host computer.
7. A method for secure provision of key credential information as defined in claim 6 comprising:
 - using the secure logic circuitry, generating display data for displaying the message prompting the user; and,
 - using a display of the secure user interface displaying the message prompting the user.
8. A method for secure provision of key credential information as defined in claim 6 comprising scanning messages

received from the remote computer for detecting the message indicative of a request for provision of the key credential information.

9. A method for secure provision of key credential information as defined in claim 7 comprising interrupting transmission of keystroke signals from a keyboard connected to the host computer to the circuitry of the host computer.

10. A method for secure provision of key credential information as defined in claim 6 comprising:

interrupting communication between the circuitry of the host computer and the remote computer after detection of the message indicative of a request for provision of the key credential information; and,

enabling the communication between the circuitry of the host computer and the remote computer after provision of the key credential information to the remote computer.

11. A method for secure provision of key credential information as defined in claim 6 comprising using the secure logic circuitry, encoding the key credential information for provision of the same in an obfuscated fashion.

12. A device for providing secure key credential information comprising:

key credential information request detection means connected to a host computer adapted for detecting a message received from a remote computer connected to the host computer and indicative of a request for provision of the key credential information;

secure logic circuitry for being disposed within the host computer and adapted for receiving key credential information from a user and providing same to the remote computer while not providing key credential information to any other processor of the host computer; and

keyboard means adapted for receiving the key credential information from the user and providing the same to the secure logic circuitry.

13. The device according to claim 12 having display means connected to the key credential information request detection means and adapted for generating a message for prompting the user for provision of the key credential information in response to the detection of a message received from the remote computer connected to the host computer and indicative of a request for provision of the key credential information.

* * * * *